DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5717

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SECURING SMART HOMES USING FACE RECOGNITION TECHNIQUES

Ishita Kumar,Yash Kothari, Harshil Kapoor, Anuraj Bhatnagar and Prof. Payal Mishra
Department of Computer Engineering
SVKM NMIMS' Mukesh Patel School of Technology Management and Engineering
Maharashtra, India

Abstract: Smart Home Technology is advancing at an exponential rate. Smart homes are no different from a small corporate network, and as such, they need similar levels of security, especially when we consider the growing trend of working from home. Smart homes need a smart Security device. With the implementation of Biometric devices, one can secure their houses as long as ensure their devices are protected of intrusion by unknown sources. Facial recognition technology has many important applications in home automation as well as in other sectors. a. It plays a key role in home automation by keeping one's home secure. An advanced facial recognition technology will be able to recognize the moment it spots one's face.

Keywords: Face recognition, Face detection, Fingerprint sensing, Raspberry Pi

I. INTRODUCTION

We can define biometrics as the science of recognizing the identity of a person based on the physical or behavioral attributes of said individual such as fingerprints, face, iris and voice. Our primary aim to deploy this project is to provide homeowners with an innovative way of securing their home devices. This project proposes to bring about a change in the biometric identification protocol by enforcing facial recognition.

The increasing use of computers and the Internet has resulted in a corresponding increase in cybercrime. This derives the need to deploy computer security. A computer security system should be able to provide some kind of information assurance such as confidentiality, integrity, availability, authenticity and non-repudiation of data.

With our project, we hope to provide owners of various electronics or devices with a way to monitor their devices remotely. One can have a complete reference to whether their device has been used and who has used it. By using the face recognition technology, faces are mapped with a unique ID. This ID will be communicated to the owner. This not only enables the user to know of the person using their device, but also how many times it is being used. This feature can be exploited to provide statistics to the user about how productive their device is by tracking, monitoring, and analyzing its use. Temporary authorizations stand out as a useful benefit of biometric locks. A given person can be given authorization on a temporary basis after which it fails to exist.

The obvious advantage of biometric technology compared to more conventional or traditional authentication methods in smart homes, such as personal ID cards, magnetic cards, keys or passwords, is that it is intrinsically linked to an individual person and therefore not easily compromised through theft, collusion or loss.

Even though there are still many concerns such as information privacy, physical privacy and religious objections, the fact cannot be denied that this technology will change our lives for the better.

We have analyzed and reviewed some research papers during the course of our literature survey, and have proposed a system based on what we have learned and observed from their contents.

II. RELATED WORK

A. The Need Of Securing Smart Homes

Smart homes constitute a branch of ubiquitous computing that involves incorporating smartness into dwellings for comfort, healthcare, safety, security, and energy conservation. They offer a better quality of life by introducing automated appliance control and assistive services. They optimize user comfort by using context awareness and predefined constraints based on the conditions of the home environment [1]. Thus, comes the need for securing them. As smart home devices are always on the path of changes, it becomes of utmost importance to provide a secure way of accessing them.

B. Face Recognition

Due to the significant advances in technology, face recognition algorithms have evolved gracefully. The significance of face recognition is due to its technical challenges and wide potential application. The first popular face recognition technique is Eigen face (Principal Component Analysis) [2]. It is a single layer model. This algorithm reflects great performance and efficiency with its functioning. Illumination, Expressions and pose do pose a challenge to the efficiency of the model. However, for a given environment with comfortable input factors, this should not hinder the working of our system.

III. PROPOSED METHODOLOGY AND SYSTEM DESIGN

With a view to provide solutions to the smart home security domain, we propose an Eigen face approach to detect and recognize faces for providing authorization. The

Raspberry Pi will be used in this approach. It will be connected to a central MODEM (Modulator and demodulator) for internet connectivity to let the user know the credentials of the person accessing his device and thereby approve or deny access to the same.

In order to test the accuracy of our model we propose to add Gaussian and poison noise in the existing database. We use the standard AT&T database due to its multifarious positioning of subjects for training and testing purposes. Our database is doubled due to the inclusion of noisy images. This report increases the accuracy of our model exponentially. Fig 1 demonstrates the overview of the proposed approach.

The details of the approach are as following:

A. 1) After the camera module is initialized subject can take his snapshot through the Raspberry Pi

B. 2) The face can be detected via Haar cascades Eigen face value

C. 3) 10 Images of each subject stored in a folder labeled testing folder

D. 4) A training set is developed with the test subjects of the AT&T database

E. 5) The images are subjected to noise. It can be

F. a. Poisson Noise,

a. b. Gaussian Noise.

b. 6) The original set and distorted set and combined and a cluster set is used as training database. Thus our training set contains twice as many images

a. 7) This cluster is given as input to the PCA Analysis module.

a. 8) The testing set is then recognized with the above trained
Network.

9) The output of the testing database is produced by comparing its results.

10) The percentage of recognition rate is calculated based on the number of correct matches with respect to total number of test images.

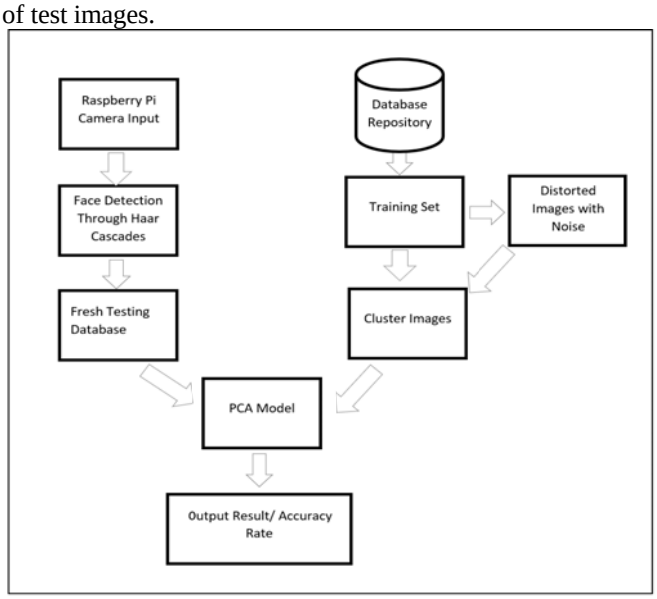

Fig 1. Block Diagram of system Design

A. Principal Component Analysis

We use the Principal Component Analysis Algorithm for the recognition of Faces. The PCA Methodology proposed the use of a Mathematical Procedure that converts a series of correlated variables into uncorrelated variables. Due to the presence of a myriad of input images and subsequent face recognition algorithms used here is Principal Component Analysis (PCA). It involves a mathematical procedure that transforms a number of possibly correlated variables into a number of uncorrelated variables called principal components, related to the original variables by an orthogonal transformation [3]. The Eigen face approach helps reducing the size of the database required for recognition of a test image.

The methodology can be explained through the flowchart mentioned in Fig 2. The key processes include:

Step 1. Prepare the training faces Obtain face images I1, I2, I3, I4, ...IM (training faces).

Step 2.The training Faces must be Centered and of the same size.

Step 3. In this approach each image of the vector M*N is converted into MN*1

Step 4. The Average Face Vector is calculated

Step 5. Each average Face vector is subtracted from every image

Step 6. Covariance Matrix is calculated

Step 7. The eigenvalues and Eigen vectors are calculated

The Eigen values calculated from the Eigen Vector covariance matrix are rejected or stored depending upon the threshold thus creating a face space. Calculating the weights and the Euclidean distance a comparison is held and match is found [5]. This conventional Eigen face Approach is incorporated in the ARM Cortex of Raspberry Pi for face recognition using face recognition modules in python code.

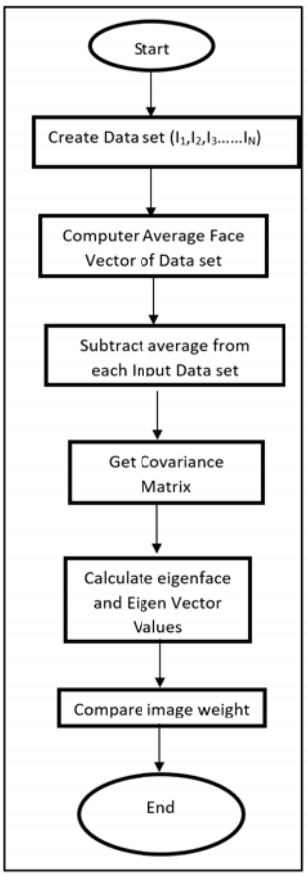

Fig2. Flow Diagram of PCA Approach

IV. SYSTEM DESIGN

A. Hardware Specifications:

The hardware specifications include:
Raspberry Pi 2 Kit, camera module, LAN Cables, Connection wires (Both Male and Female), LCD, USB Keyboard, USB Mouse and Power Supply.
Raspberry Pi 2:
The raspberry pi is a microprocessor or rather a small-scale computer. At the mere size that fits in the palm, it offers the utility of a personal computer for coders and developers.
The Raspberry pi offers software's to users such as RASPBIAN, PIDORA, OPENELEC, RASPBMC, RISC OS, and ARCH LINUX. All these software's can be downloaded easily and for free from the official forum under the NOOBS (new out of the box software) category [3]. It contains the following components: I/O Port, the RAM, CPU and GPU, Several USB Hubs, Ethernet and HDMI Port.

B. Software Specifications:

Open CV and Visual studio are the basis of our design module. Within Visual studio, we use the C# language.

Open CV
Open CV or Open Computer Vision is a leading library for developers in the domains of Image processing, Object detection and Machine learning. In our project we import open CV's Python libraries in our Project. Libraries such as EmguCv are used for the same.

Visual Studio
Visual studio is an Integrated Development Environment that endeavors to help developers design their own software's. The designing of our project is on the Visual Studio in C#. With the various libraries imported from OpenCv, we propose to make a user-friendly UI design.

AT&T Database:
Testing of our project is carried out on the AT&T face database. The dataset contains forty subjects, with each subject having ten image samples of size 112 X 92 each. We modify the original database by adding synthetic image samples. Imposing the input samples with noise does this. We use two noise functions. The Gaussian noise and the Poisson noise. The former imparts more variation of distortion that the latter.

V. EXPERIMENTAL ANALYSIS AND RESULT

In this section the above explained approach of using PCA analysis. As our implementation is visual studio centric, the user Interface is made keeping the ease of use in mind.
Poisson noise or rather shot noise is a type of electronic noise that is modeled during any Poisson process whereas Gaussian noise, the values that can be substituted are Gaussian distributed. Gaussian noise is subjected to more distortion as compared to Poisson noise with a mean of 0 and a variance of 0.01

Using these two image noise features we test the accuracy of our model. The synthetic images developed are tested as training images. Testing images may also be subjected to noise to test the real time accuracy of the system. Fig shows the training set, which is subjected to Gaussian noise and Poisson noise respectively.

Fig 3.Row 1:Training images of original subject in AT&T database, row 2: Gaussian noise applied to the subject, and row 3: Poisson noise applied to the subject. All columns have the same person with variation of Poses.

We may also subject the real time testing faces to Gaussian and Poisson noise.

Fig 4: Row 1: Real-time testing images of original subject in AT&T database, row 2: Gaussian noise applied to the subject, and row 3: Poisson noise applied to the subject. All columns have the same person with variation of Poses.

The performance metric of our system is the accuracy of our system, which is calculated as the ratio of correct matches to the total matches.

Table 1: Accuracy of Data

Training Set	Total number of Images of one subject	Number of Subjects in Database	Average Rate of Match
Original	10	10	9
With Gaussian Noise	10	10	6.5
With Poisson Noise	10	10	7.8

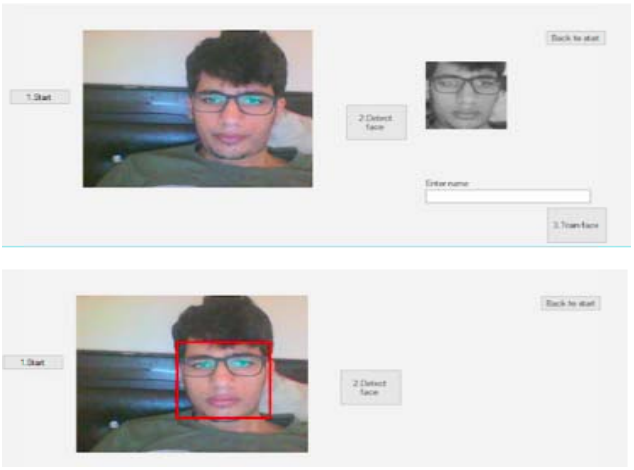

Fig5. Working of Module

Images with Poisson noise serves to offer more accurate matches as compared to Gaussian Noise. This may be due to the factor that Poisson noise has seemingly lesser electric noise distortion as compared to Gaussian noise.

VI. CONCLUSION

Biometrics alludes to automatic recognition of an individual considering her behavioral as well as physiological qualities. The ordinary knowledge based, and token-based methods do not really provide positive personal recognition since they depend on surrogate representations of the person's identity. It is subsequently clear that any system assuring reliable personal recognition must necessarily involve a biometric component.

Biometric- based frameworks additionally have a few impediments that they have unfriendly ramifications for the security of a system. There are various security concerns raised about the utilization of biometrics. A sound trade-off amongst security and privacy might be essential.

VII. FUTURE SCOPE

The Principal Component analysis model, while a very accurate model does not provide complete security when it comes to face recognition. We may improve the efficiency by turning towards Artificial Neural Networks.

High-dimensional data can be converted to low-dimensional codes by training a multilayer neural network with a small central layer to reconstruct high-dimensional input vectors [6]. More than one type of Biometric can also be incorporated in order to increase the accuracy of system. Multimodal biometric systems are more reliable due to the presence of different modals, which meets the requirements imposed by various applications. Multi-biometric systems have recently been proposed where a decision is made based on a fusion or combination of different subsets of biometrics. It is relatively difficult to spoof multiple biometrics simultaneously [7]. Smart homes can be made even smarted by incorporating alerts to device user when the Device is being used. This can be executed by adding a few lines of code and importing the SMTP library that can send e-mail with the help of the SMTP (Simple Mail Transfer Protocol) [8].

REFERENCES

[1] Muhammad Raisul Alam, Student Member, IEEE, Mamun Bin Ibne Reaz, Member, IEEE, and Mohd Alauddin Mohd Ali, Member, IEEE "A Review of Smart Homes—Past, Present, and Future" ieee transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 42, no. 6, november 2012.

[2] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," In *Computer Vision and Pattern Recognition*, pages 586–591, 1991.

[3] Pritish Sachdeva and Shrutik Katchii, "A Review paper on Raspberry Pi" Proceedings International Journal of Current Engineering and Technology, IJCET-14Y

[4] [4]. Katchii, "A Review paper on Raspberry Pi" Proceedings International Journal of Current Engineering and Technology, IJCET-14Y

[5] G. Hu, X. Peng, Y. Yang, T. Hospidales, and J. Verbeek."Frankenstein: Learning Deep Face Representations using Small Data," arXiv:1603.06470v2, 2016

[6] G.E Hinton and R.R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, 313(5786):504–507, 2006

[7] M. S. Islam n, R. Davies, M. Bennamoun, R. A. Owens, A. S. Mian, "Mult ibiometric human recognition using 3D ear and face features", www. elsevier. com/locate/pr(2012)

[8] Yashwanth Sai, Vijai Chandra Prasad, Niveditha .P., Sasipraba , Vigneshwari and S.Gowri, "Low cost automated Facial Recognition system"